Secure boot vulnerability demonstrator (AISEC)

Secure boot is a fundamental building block to build secure embedded systems. Key element of a secure boot in embedded systems is the hardware root of trust: An immutable ROM code that uses a public key to verify the first stage boot loader, starting the chain of trust. However, if the SoC’s ROM code itself suffers from vulnerabilities, the whole secure boot may be broken beyond any repair, as the silicon’s ROM code is unpatchable. In this work we will setup a demonstrator to show a known secure boot vulnerability in a ROM boot code of a real world SoC.

Prerequisites

The following skills are valuable for the execution of the project:
* Experience with embedded Linux
* Basic knowledge of programming in C
* Knowledge about embedded security, e.g., from a lecture
* Experience in using Git
* Structured way of working and being able to work independently

Contact

If you are interested in this position, please send an email with
* a short CV,
* a short cover letter, and
* your last grading sheet.

Kilian Zinnecker, kilian.zinnecker@aisec.fraunhofer.de

Advisors

Georg Sigl
Kilian Zinnecker (Fraunhofer AISEC)